Patent claims

1. Method for forming a secrete communication key for a predetermined asymmetric cryptographic key pair, which comprises a secrete key and a corresponding public key, by a computer,
a) whereby a prescribable initial value has been used given the determination of the key pair,
b) whereby the initial value is made available to a user,
c) whereby the user enters the initial value into the computer,
d) whereby the secrete communication key is formed upon utilization of the initial value, whereby the secrete communication key and the public key form an asymmetric cryptographic communication key pair.

2. Method according to claim 1,
whereby the initial value is supplied to a hash function and the value formed by the hash function is used for determining the key pair and the communication key pair.

3. Method according to claim 1 or 2,
whereby additional data characterizing the user are utilized when the key pair and the communication key pair are formed.

4. Method according to one of the claims 1 to 3,
- whereby a prime number is determined on the basis of the initial value, whereby, in an iterative method, it is checked whether the respectively checked number is a prime number and when this is the case, an index is stored, which refers to a plurality of numbers, which have been checked with respect to their property whether they are a prime number, is stored [sic],
- otherwise, another number is selected on the basis of the checked number and the index is increased by a prescribed number,

- whereby the used prime number is erased after the communication key pair has been formed,

whereby the index and the initial value are respectively used for forming a new communication key pair for forming the secrete communication key.

5. Method according to claim 4,
whereby the test, whether a number is a prime number, is carried out according to the method of Miller-Rabin.

6. Method according to one of the claims 1 to 5,
whereby the keys are formed according to the RSA method.

7. Method according to one of the claims 2 to 6,
whereby the hash function is one of the following methods:

- MD-5 method,
- MD-2 method,
- the method according to the Data Encryption Standard (DES) as one-way function.

8. Method according to one of the claims 1 to 7,
used for enciphering electronic data with the secrete communication key.

9. Method according to one of the claims 1 to 7,
used for forming a digital signature via electronic data upon utilization of the secrete communication key.

10. Method according to one of the claims 1 to 7,
used for authenticating upon utilization of the secrete communication key.

11. Arrangement for forming a secrete communication key for a predetermined asymmetric cryptographic key pair, which comprises a secrete key and a

corresponding public key, with a processor being set up such that the following steps can be carried out:

- the key pair has been determined upon utilization of a prescribable initial value,
- the initial value is made available to a user,
- the user enters the initial value into the computer,
- the secrete communication key is formed upon utilization of the initial value, whereby the secrete communication key and the public key form a communication key pair, and

with an input means for entering the initial value by the user.

12. Arrangement according to claim 11, whereby the processor is set up such that the initial value is supplied to a hash function and the value formed by the hash function is used for determining the key pair and the communication key pair.

13. Arrangement according to claim 11 or 12, whereby the processor is set up such that additional data characterizing the user are utilized during the formation of the key pair and the communication key pair.

14. Arrangement according to one of the claims 11 to 13, whereby the processor is set up such that

- a prime number is determined on the basis of the initial value, whereby, in an iterative method, it is checked whether the respectively checked number is a prime number and when this is the case, an index is stored, which refers to a plurality of numbers, which have been checked with respect to their property whether they are a prime number, is stored [sic],
- otherwise, another number is selected on the basis of the checked number and the index is increased by a prescribed number,
- whereby the used prime number is erased after the communication key pair has been formed,

- whereby the index and the initial value are respectively used for forming a new communication key pair for forming the secrete communication key.

15. Arrangement according to claim 14,
whereby the processor is set up such that the test, whether a number is a prime number, is performed according to the method of Miller-Rabin.

16. Arrangement according to one of the claims 11 to 15,
whereby the processor is set up such that the keys are formed according to the RSA method.

17. Arrangement according to one of the claims 12 to 16,
whereby the processor is set up such that the hash function is one of the following methods

. Method according to one of the claims 2 to 6,
whereby the hash function is one of the following methods:

- MD-5 method,
- MD-2 method,
- the method according to the Data Encryption Standard (DES) as one-way function.

18. Method according to one of the claims 11 to 17,
used for enciphering electronic data with the secrete communication key.

19. Arrangement according to one of the claims 11 to 17,
used for forming a digital signature via electronic data upon utilization of the secrete communication key.

20. Arrangement according to one of the claims 11 to 17,
used for authenticating upon utilization of the secrete communication key.